



MANUAL DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PARA FORNECEDORES

AFEAM

EMISSÃO 06 DE MAIO DE 2019.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PARA FORNECEDORES - PSIC

1. Objetivo

Declarar formalmente, por meio da sua Diretoria, as diretrizes da AFEAM que visam à proteção dos ativos de informação com eficiência, eficácia e competitividade, de modo seguro, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade, assim como dos ativos de tecnologia de informação que as sustentam, de forma alinhada aos requisitos legais e exigências dos órgãos regulatórios de acordo com o negócio.

Estabelecer as competências, responsabilidades e limites de atuação dos fornecedores e prestadores de serviços da AFEAM, em relação à segurança da informação e cibersegurança, reforçando a cultura de segurança e priorizando as ações necessárias conforme o negócio.

Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético da AFEAM.

2. **Regulamentação:** Resolução nº 4.658/2018, do Banco Central do Brasil.
3. **Periodicidade de revisão:** no mínimo anualmente, ou, extraordinariamente, a qualquer tempo.
4. **Interpretação:** Esta PSIC e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização, devendo ser levada em consideração a análise de risco (GECOR) e a necessidade do negócio à época de sua solicitação.
5. **Propriedade:** As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos prestadores de serviços e fornecedores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade e direito de uso exclusivo da AFEAM e devem ser empregados unicamente para fins profissionais.
6. **Classificação da Informação:** Os prestadores de serviços e fornecedores devem utilizar apenas os recursos disponibilizados pela AFEAM para classificar a informação e aplicar os respectivos controles estabelecidos em documento específico, em todo o ciclo de vida da informação, ou seja, desde a sua recepção ou produção até o seu descarte.
7. **Sigilo:** É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade da AFEAM, por seus prestadores de serviços e fornecedores, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja classificada como “pública”.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PARA FORNECEDORES - PSIC

8. **Uso dos Ativos de Tecnologia da Informação:** Os ativos de informação de propriedade da AFEAM devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.
9. **Autenticação:** O prestador de serviço e fornecedor é responsável pelo uso e sigilo de suas credenciais de acesso, onde não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de credenciais de terceiros, sendo responsável direto pela conduta ou/e dano causado, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.
10. **Criptografia:** A AFEAM estabelecerá critérios para a implantação de ferramentas de criptografia, além de garantir o seu uso efetivo e adequado, com o intuito de garantir a segurança das informações na Instituição.
11. **Prevenção e Detecção de Intrusão:** A AFEAM possui ferramentas para realizar monitoramento e análise de eventos em sistemas computacionais, com o propósito de detectar e prover alertas sobre tentativas de acesso não autorizado a recursos destes sistemas.
12. **Prevenção de vazamento de informações:** Arquivos contendo dados sensíveis da AFEAM, quando transferidos de qualquer forma pela internet, devem estar protegidos de vazamento, adulteração e outras ameaças à integridade e confidencialidade da informação
13. **Estabelecimento de mecanismos de rastreabilidade:** O uso dos recursos de tecnologia da informação e comunicações disponibilizados pela AFEAM é passível de monitoramento, rastreamento e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade, através utilização de solução DLP.
14. **Controle de acesso:** A AFEAM controla o acesso físico e lógico às suas dependências e aos seus ativos de informação. Desse modo, cada prestador de serviço e fornecedor deve possuir uma credencial de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.
15. **Salvaguarda (backup):** A AFEAM deve definir e manter um processo de salvaguarda e restauração das informações e de seus ativos de informação críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.
16. **Desenvolvimento seguro e aquisição de software:** O desenvolvimento interno e/ou externo de softwares, assim como a aquisição de softwares e produtos no mercado, devem possuir requisitos de segurança para garantir informações confiáveis, íntegras, autênticas e oportunas.
17. **Segurança em Ambiente para Computação em Nuvem (Cloud Computing):** a AFEAM é responsável pela confiabilidade, integridade, disponibilidade, segurança e

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PARA FORNECEDORES - PSIC

pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

18. **Manutenção dos Ativos de informação:** Todos os ativos de informação em uso no ambiente corporativo da AFEAM devem atender as recomendações de seus fabricantes ou desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança.
19. **Mobilidade:** Os ativos de informação que permitem mais mobilidade ao prestador de serviço e fornecedor devem ser utilizados somente quando fornecidos ou autorizados pela AFEAM, que deve ocorrer somente após solicitação formal e fundamentada do prestador de serviço e fornecedor solicitante e autorização expressa da GECOR. Além disso, devem estar diretamente relacionados a uma justificativa do negócio, com motivo estritamente profissional, no âmbito das atribuições do prestador de serviço e fornecedor.
20. **Ativos de informação Particulares:** O uso de ativos de informação particulares na execução de qualquer atividade profissional ou na interação com os ambientes físicos ou lógicos ou com as informações da AFEAM deve ocorrer somente após solicitação formal e fundamentada do prestador de serviço e fornecedor solicitante e autorização expressa da GECOR.
21. **Repositórios digitais:** É vedado aos prestadores de serviços e fornecedores o uso de repositórios digitais (ex: dropbox, iCloud, WeTransfer, google drive), salvo casos onde seja realizada solicitação formal e aprovada pelo CSIC.
22. **Áudio, Vídeos e Fotos:** É vedada qualquer atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências da AFEAM por seus prestadores de serviços e fornecedores, inclusive no âmbito acadêmico ou uso nas mídias sociais, salvo casos onde seja realizada solicitação formal e aprovada pelo CSIC.
23. **Auditoria junto aos prestadores de serviço:** Cláusulas contratuais que dispõem sobre a realização de auditorias eventuais ou periódicas para certificar a conformidade com a PSIC devem ser estabelecidas junto aos prestadores de serviço da AFEAM.
24. **Monitoramento:** A AFEAM realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, ativos de informação e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.
25. **Capacitação:** A AFEAM possui um Programa Anual de Conscientização em Segurança da Informação e Cibersegurança para capacitação, avaliação e disseminação da cultura de Segurança da Informação junto aos colaboradores, prestadores de serviços e fornecedores.
26. **Comunicação de Incidentes:** A AFEAM deve possuir um canal de comunicação divulgado aos seus prestadores de serviços e fornecedores para reportar

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PARA FORNECEDORES - PSIC

imediatamente os possíveis casos de incidentes de segurança da informação e cibernética, podendo fazer de modo formal ou com uso do recurso de denúncia anônima.

Será realizada a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela AFEAM, bem como das providências para o reinício das suas atividades.

- 27. Alterações:** As alterações desta PSIC e de seus documentos complementares devem ser devidamente comunicadas aos seus prestadores de serviços e fornecedores pela AFEAM.
- 28. Exceções:** As exceções que ocorram de forma exclusiva e excepcional a essa PSIC, devem ser formalizadas e fundamentadas pelo prestador de serviço e fornecedor solicitante, e podem ser revogadas a qualquer tempo, por mera liberalidade da AFEAM, conforme previsto em procedimento específico. Criar procedimento ou CI de exceção.

As medidas alternativas às previstas nesta PSIC, realizadas de modo excepcional para mitigar riscos em ocasiões específicas e justificáveis, inclusive em situações emergenciais, devem ser formalizadas e fundamentadas pelo prestador de serviço e fornecedor de forma imediata ou assim que possível ao CSIC.

- 29. Violações:** As violações de segurança devem ser informadas à GETI, por meio do Help Desk ou telefone. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas.

Os princípios de segurança estabelecidos na presente política possuem total aderência da administração da AFEAM e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta política está sujeita os prestadores de serviços e fornecedores às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

Dúvidas: Qualquer dúvida relativa a esta PSIC deve ser encaminhada ao CSIC por meio do e-mail csic@afeam.org.br.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PARA FORNECEDORES - PSIC

TERMO DE COMPROMISSO PARA COLABORADORES EXTERNOS

Este Termo de Compromisso se aplica a todos os prestadores de serviços, terceirizados, conveniados, credenciados, fornecedores e clientes usuários das Informações e dos Ativos de Tecnologia de Informação e Comunicação da AFEAM.

Declaro que, na condição de colaborador externo e usuário das Informações e dos Ativos de Tecnologia de Informação e Comunicação pertencentes à AFEAM, firmo, por meio deste documento, o entendimento e a aceitação da Política de Segurança da Informação e Cibernética para Fornecedores da AFEAM, bem como dos seus documentos complementares.

Como parte deste Termo, comprometo-me a:

- a. Preservar a confidencialidade, a integridade e a disponibilidade das Informações obtidas durante a vigência da minha relação jurídica com a AFEAM, mesmo após o seu término;
- b. Manter sigilo sobre o ambiente da AFEAM e os ativos de informação fornecidos;
- c. Manter sigilo sobre informações confidenciais do negócio da AFEAM;
- d. Informar imediatamente ao departamento responsável pela gestão da relação jurídica e à Gerência de Tecnologia de Informação e Comunicação a respeito de qualquer falha, incidente ou anormalidade dos ativos de Tecnologia de Informação e Comunicação da AFEAM;
- e. Agir de forma responsável em relação aos recursos alocados para o desenvolvimento de minhas atividades profissionais.

Declaro que os Ativos de Tecnologia de Informação e Comunicação de minha propriedade, incluindo os *softwares*, trazidos por mim para a AFEAM, serão de minha exclusiva responsabilidade.

Declaro, ainda, estar ciente de que a violação a este Termo resultará nas medidas legais cabíveis.

Manaus, ____ de _____ de _____.

Unidade Gestora

Representante legal da Empresa

Nome da Empresa

CNPJ

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PARA
FORNECEDORES - PSIC**

Se pessoa física, informar nome completo e CPF

<i>NOME</i>	<i>CPF</i>	<i>Assinatura</i>